Listing Of Claims

1. (Currently Amended) A system for processing of information over a network comprising: at least first and second -processing devices and an interface, the first processing device for transmitting a communication having a desired destination being the second processing device, the first processing device also transmitting the security information associated with the communication, wherein said security information includes biometric information of the originator for identifying the originator of the communication, the communication and security information being received by the interface, ~~,~~the interface having access for processing a subset of the security information and communication to identify an authorized ~~or unauthorized~~ condition, with the interface processing the subset of security information and communication by comparing the security information against previously stored security information to determine when there is a match between the security information and stored security information indicating an authorized condition, the interface transmitting the communication to the second processing device on identification of an authorized condition~~.~~, the communication being retained at the interface or transmitted to a third secured processor on identification of an unauthorized condition, where there is no match made between the security information and stored security information, so that the communication does not reach the second processing device, the system further comprising a storage device containing the security information in electronic form that is communicated to the first processing device, wherein the storage device comprises a smart card.

2. (Cancelled)

3. (original) The system of claim ~~2~~ 1, wherein the stored security information is located in a database.

4. (Canceled)

5. (Canceled)

6. (Currently Amended) The system of claim ~~5~~1, wherein ~~the storage device comprises a card,~~ the first, ~~and~~ second and third processing devices comprises a computer and the -interface ~~comprise~~ comprises a server.

7. (original) The system of claim 6, further comprising a reader in communication with the first processing device and adapted to upload the security information from the card and download the security information onto the first processing device.

8. (original) The system of claim 6, wherein the first processing device transmits the communication and security information over a network.

9. (original) The system of claim 8, wherein the network comprised the internet .

10. (original) The system of claim 8, further comprising at least one of an IP address of the computer or a GPS tracking device on at least one of said card, reader or computer for providing location information.

11. (Currently Amended) The system of claim 10, wherein the card comprises a plurality of independent compartments, in which each compartment comprises memory that stores ~~contains~~ different preselected categories of information, and with each compartment ~~requires~~ containing a different unique arrangement of pin codes located on the card and which can communicate with one or more readers having a similar arrangement of pins codes provided thereon for ~~access thereto~~ uploading or downloading of information.

12. (original) The system of claim 11 in which said card displays a photo image of the person assigned to said card.

13. (original) The system of claim 12 in which said card contains in a compartment a digitized photo image of the person assigned to said card.

14. (original) The system of claim 13 in which one of said compartments contains biometric identifying information about the assigned user of said card.

15. (Currently Amended) The system of claim 8, wherein the communication comprises an electronic mail communication-.

16. (Currently Amended) The system of claim 15, wherein the biometric information –selected from the group consisting of facial characteristics, finger prints, DNA, and retina characteristics.

17-33. (Canceled)

34. (Currently Amended) A method of information processing comprising:

storing identifying information on a card, wherein said identifying information comprises biometric information including fingerprint information for identifying an owner of the card;

reading the stored identifying information from said card;

creating an authentication mark based at least in part on the ~~stored~~ read identifying information;

transmitting information along with the authentication mark-;

receiving the information along with the authentication mark at a first destination;

verifying whether the information is authorized based on the authentication mark and a subset of the information; and

transmitting authorized information to a second destination.

35. (original) A method of claim 34, further comprising measuring actual identifying information, comparing the measured actual identifying information against the stored identifying information and transmitting the information and authentication mark where there is a match between the measured actual identifying information and stored identifying information.

36. (Canceled)

37. (Currently Amended) The method of claim ~~36~~ 34, further comprising basing the authentication mark on the biometric information.

38. (Currently Amended) The method of claim 37 further comprising providing a reader for reading the stored identifying information, a biometric device for measuring the actual biometric information -and a computer for transmitting the information and authentication mark over a network.

39. (original) The method of claim 38, further comprising basing the authentication mark on location information of the computer.

40. (original) The method of claim 39, wherein the location information comprises at least one of an IP address of the computer or a GPS tracking device on at least one of said card, reader or computer for providing the location information.

41. (Currently Amended) The method of claim 40, further comprising transferring of the authentication mark and information transmitted from the computer to one or more target computers external to the computer-.

42. (Currently Amended) The method of claim 41, further comprising regulating access to the one or more target computers based on the authentication mark.

43. (original) The method of claim 37, wherein verifying whether the information is authorized based on the authentication mark comprising comparing the biometric information from the authentication mark against stored biometric information.

44. (New) A computer-readable medium having computer-executable instructions for performing steps comprising:

receiving a data communication comprising biometric information for a user at a device for storing said data;

comparing a subset of said data communication with locally stored information; and

enabling further transmission of said data communication when a match is found between said received data communication and said locally stored information.

45. (New) The computer-readable medium of claim 44, further comprising enabling the further transmission of another data communication associated with said received biometric information.

46. (New) The computer-readable medium of claim 45, further comprising preventing the further transmission of said data communication when a match is found between said data communication and pre-determined computer virus or worm characteristics.

47. (New) The computer-readable medium of claim 44, wherein said data communication comprises location information for the device for storing said data.

48. (New) The computer-readable medium of claim 47, wherein said location information comprises an IP address.

49. (New) The computer-readable medium of claim 44, wherein said biometric information comprises at least one of a facial characteristic, finger print, DNA identifier or retina characteristic.

50. (New) The computer-readable medium of claim 44, further comprising determining a subset of said received data communication for comparison with locally stored information based on a pin code associated with said locally stored information.

51. (New) The system of claim 1, wherein the security information further comprises a designated security clearance level, with higher security clearance levels having authorization to access the second processing device and lower security clearance levels not having authorization to access the second processing device, wherein the interface identifies the designated security clearance level on receipt of the security information, and on detection of higher security levels transmits the communication to the second processing device, and on detection of lower security clearance levels retaining the communication at the interface or transmitting the communication

to a third secured processor, so that the communication does not reach the second processing device.

52. (New) The system of claim 51, wherein the interface further processes the communication for detection of any problems, wherein the problems are selected from the group comprising viruses, worms or illegal/immoral subject matter.

53. (New) The system of claim 52, wherein on detection of any problems, the interface transmits the identifying information of the originator to authorities.

54. (New) The system of claim 8, further comprising a GPS tracking device on at least one of said card, reader or computer for providing location information comprising the place from where the communication originated and time of the transmission, and with said location information being incorporated into the communication and security information transmitted.

55. (New) The method of claim 40, wherein the location information comprises the GPS tracking device, with the location information comprising the place from where the communication originated and time of the transmission, and with said location information being incorporated into the authentication mark.